EXHIBIT A

WILSON ELSER
WILSON ELSER MOSKOWITZ EDELMAN & DICKER LLP

Aaron Weissberg
Associate
Tel: (914) 872-7189

November 20, 2018

Via Email and First Class Mail

Brian L. Bromberg [brian.bromberg@gmail.com]
Bromberg Law Office, P.C.
Standard Oil Building
26 Broadway, 21st Floor
New York, New York 10004

Even Weissman [eve@neweconomynyc.org]
New Economy Project
121 W. 27 Street, #804
New York, New York 10001

Re: Ruane v Bank of America, N.A. and Chex Systems, Inc. – 17-CV-3704

Dear Mr. Bromberg and Ms. Weissman:

While we await our client's confirmation of additional draft responses we have prepared based upon the information they have provided which we hope to have tomorrow, we are providing you with this specific response as to the nature of Bank of America, N.A.'s investigation and the basis for its conclusions. This is our client's response according to Bank of America, N.A. ("BANA"), it is as follows:

It is BANA's position that after investigation and re-investigation, it reached a reasonable and good faith conclusion supported by demonstrable facts that Plaintiff was complicit with a third party perpetrator who Plaintiff assisted by providing her account information and access to the perpetrator in return for financial benefit. This scenario is a known "sold account" scam perpetrated upon financial institutions with which BANA's fraud investigators are well familiar. BANA's investigation and conclusions involved a specific and discrete set of facts and attendant circumstances as to the Plaintiff and the account transactions, all as will be further discussed herein.

Facts and Sequence of Events

The chain of events began after five counterfeit checks were deposited via a Samsung Android mobile device with an IP address located in Illinois on 9/27/16, using established log-in ID credentials for Adiaha Ruane. The counterfeit checks were first immediately identified by BANA's automated fraud detection system upon their deposit and were routed for additional review as will be further discussed herein. As a result of the observed fraudulent activity involving the Account,

a hold was placed by BANA for the funds represented by the spurious checks and the Account was subsequently closed and reported to Chex Systems. According to BANA, activity associated with the account is consistent with a so-called "Sold Account" fraud trend in which customers actively participate in committing fraud against the bank by providing account credentials to a third party fraudster, permitting customer accounts to be used for fraudulent activity in return for financial benefit. Plaintiff generally maintained insubstantial balances in her BANA account and may also have had other financial pressures, including without limitation, apparent entered judgments against her by third parties that would have been motivation enough for the selling of her account information.

On 9/26/16, Plaintiff's ending daily account balance was $67.52. Plaintiff's average daily balance for the previous month was $198.

On 9/27/16, the five subject checks totaling $4,838.97 were deposited into Plaintiff's account using a Samsung Android mobile device (with T-mobile as the provider), using Plaintiff's established multiple, layered log-in credentials consisting of Plaintiff's correct ID, password, and correctly answered challenge questions which only Plaintiff would have known. The challenge questions were:

Q1. What was the name of your first pet?

Q2. In what city were you married?

Q3. In which city did you meet your spouse for the first time?

Significantly, Plaintiff had set up Fingerprint ID on her iPhone 6s. The foregoing challenge questions are only asked if a Finger ID is not set up on the particular device that is attempting to access a BANA customer account. In the case of Plaintiff, only the iPhone 6S belonging to Plaintiff was set up for Finger ID. Consequently, when the unrecognizable Samsung Android device attempted to access Plaintiff's account online, the challenge questions acted as extra layers of security insulation in addition to Plaintiff's user ID and password to verify that it was indeed Plaintiff accessing her account on a different device. The challenge questions were all correctly answered using the Android device. This is plain proof that someone other than Plaintiff, located in Illinois and using another device not set up with Plaintiff's Fingerprint ID accessed Plaintiff's account using personal account information disclosed by only Plaintiff herself.

Based on BANA's records, the Samsung Android device appeared to have accessed Plaintiff's BANA account on 9/27/16 and 9/28/16 from an IP address in Illinois.

The first spurious check was deposited at 6:02 pm EST, followed quickly by the second, third, fourth and fifth checks deposited between 8:29 pm and 8:43 pm EST --- all on 9/27/16. The Account was then accessed clearly by Plaintiff a total of eleven times following the first deposit using her e-mobile device and her fingerprint ID (five times on 9/27/16 and six times on 9/28/16). As a result, Plaintiff was clearly viewing the account deposits as pending deposits.

On 9/27/16 at 8:40 pm EST, the deposit of the checks triggered BANA's automated fraud detection alert as each check had the same maker/routing and transit information and the available balance

at the time of deposit was less than $500. The alert resulted in the referral of the suspect transactions for manual review the very next morning by a BANA fraud investigator. [1]

On 9/28/16 at 10:44am EST, Fraud Detection Analyst, Adrianna Mendoza reviewed the automated alert and made a recommendation to close the Account based on (i) her review of the imaged deposits and (ii) her fraud investigation check list comprised of the following factors:

- Customer's relationship and length of relationship with the Bank (customer since 2005),
- Customer's transactional history (balances, purchases, deposits, returned items),
- Method of questionable deposit (via ATM, mobile device, Financial Center),
- Device login history (including device, location, frequency & recency of access)
- Other account maintenance events that are red flags for potential identity theft (including recent address change, phone number change, OLB ID change, OLB password change, etc.)

It is important to note that Ms. Mendoza would have also been on the lookout for "Account Takeover" risk factors on the Account prior to closing the Account. In considering whether this situation was one of account takeover, Ms. Mendoza analyzed the Account for non-monetary changes or patterns such as changes to account access information like address of record, passwords and challenge questions. However, in this situation, those benchmarks and patterns were absent as to Plaintiff's account. The account information did not change and Ms. Mendoza did not see a pattern of non-monetary account changes, consequently Ms. Mendoza then turned to her analysis from a "sold account" scam perspective.

At the conclusion of her review, Ms. Mendoza made a recommendation to her supervisor, Senior Fraud Detection Analyst, Juliana Yao to close Plaintiff's account. Ms. Mendoza reviewed all of the factors mentioned above with Ms. Yao. Most pertinent was the observation that on the day of the deposits, Plaintiff accessed the account via the iPhone 6S mobile device 13 times, a behavior inconsistent with Plaintiff's history of an average of 2.1 times per day over the prior 90 day window. On the day of the deposits, Plaintiff accessed the account 8 times prior to the first deposit and 5 times after the first deposit. Plaintiff also accessed the account 7 times the following day. (beginning at 12:16 AM EST, 1:25 am EST, and 1:52 am EST, 8:45 am, 9:45 am EST, 10:43am EST and 10:51am EST) using established login credentials & fingerprint ID. Plaintiff even accessed the account via her iPhone 6S at the same time as the Samsung Android was actively in session as the first counterfeit deposit was submitted.

Following Ms. Mendoza's recommendations to her supervisor, Ms. Yao, to close the Account, that same morning of 9/28/18, Ms. Yao conducted her evaluation of the suspected fraud transactions and Plaintiff's involvement and concurred with Ms. Mendoza's findings and conclusions. Based upon the observations made of the activity on the Account and the foregoing attendant events, Ms. Yao recommended that the Account be sent to BANA's Account Closure team in order to close down the account and report it to Chex Systems. At this point in time, Plaintiff's access to her online banking would have been blocked by BANA.

Communications from Plaintiff

[1] Funds deposited prior to 9 PM EST are typically available the next business day, but the fraud alert prevented the pending fraudulent deposit funds from being reflected as "available" to Plaintiff, a fact visible to Plaintiff while she was on her on-line banking sessions as noted above.

Plaintiff's first contact with BANA

On 9/28/16 at 11:25 am EST, some 10 minutes after BANA blocked access to the Plaintiff's online banking facility, Plaintiff called BANA for the first time since the counterfeit check deposits and spoke with a BANA Customer Service Center representative, Abria Boykin -- but significantly BANA's records confirm that the sole item of discussion was simply Plaintiff's request to re-set her online banking password, with no mention by Plaintiff of the fraudulent check deposits despite having been viewing those transactions as noted above. At 12:38 pm EST, Plaintiff again called BANA to reset her online banking password and spoke with another customer representative, William Tolbert, who transferred the call to the account closure team for further assistance. David Treto of the Account Closure team handled this transferred call at 12:41pm EST. BANA does not have a recording of the calls given the timeframe. At 1:16 pm EST, Plaintiff made another call and spoke to customer representative Eusebio Orozco. This call was also transferred to Fraud Claims. However BANA's record reflects that Plaintiff did not assert or request to file any claim regarding the clearly counterfeit checks or raising any issue as to those checks.

Examination of Plaintiff's Account

Online Account Access and Activity

Typically, Plaintiff accessed her online banking account using phone number 718-954-1518, with Sprint Spectrum/Sprint PCS as her telephone provider. According to BANA this number was also the phone number provided on her account profile. As discussed above, the subject check deposits were made using a Samsung Android mobile device from an IP address in Illinois.

Account activity

As noted above, prior to the deposit of the subject checks, the ending daily account balance was $67.52. The ending balance on the day of closure was $22.36, excluding the counterfeit deposits. Although the account was 'suspended', access to existing funds as well as new direct deposited funds continued to be permitted. Plaintiff was able to withdrawal all funds on 10/5/16.

On 9/29/16, BANA rejected all of the subject counterfeit checks that had been deposited, resulting in a small overdrawn position until another direct deposit was received on 9/30/16, putting the account into a small positive balance position.

On 9/30/16 at 11:54 am, Plaintiff called BANA's customer service team and spoke with Roxanne Green (an associate with a third party vendor (ACCT Holding) providing such services to BANA). BANA's records indicate that Plaintiff simply requested to have her account funds released, but was advised that the process would take 24-72 hours.)

Apparently as part of Plaintiff's effort to obtain the release of her remaining legitimate account funds, including her anticipated monthly pension payment which was received and credited, there ensued another series of communications as follows:

On 10/1/16 at 12:17 pm, Plaintiff called and spoke with Sara Prado (another employee of the above third party vendor). Plaintiff called again at 4:40 pm and spoke with Christopher Foust (another employee of the above third party vendor). No notes or recordings exist of the substance of those two calls.

WILSON ELSER

On 10/3/16 at 11:30am, Plaintiff called and spoke with Maria Magdale Long (another employee of the above third party vendor). No notes or recordings exist of the substance of that call.

On 10/5/16 at 3:08 pm, Plaintiff spoke with Amy Probert (Retail Contact Center). No notes or recordings exist of the substance of that call.

On 10/5/16 at 3:17 pm, Plaintiff called and spoke with Jonathan Hernandez (a vendor employee with Teletech. Plaintiff completes a withdrawal at a BANA financial center for the remaining balance in her account. Thereafter, BANA formally closed out Plaintiff's account on its system as of 11/1/16.

On or about 3/16/17, BANA received Plaintiff's correspondence disputing BANA's reporting of Plaintiff to Chex Systems. Plaintiff claimed that she did not deposit the counterfeit checks and requested that BANA correct its adverse reporting based upon the transactions. On 3/17/17, Chex Systems electronically sent to BANA a request for reinvestigation of BANA's reporting as to Plaintiff.

On 4/8/17, after such re-investigation based upon a review of all the information and circumstances it had considered in filing its initial report, BANA confirmed to Chex Systems that the report was correct. It is noteworthy that the received re-investigation request provided no new facts and BANA determined that its original decision was appropriate.

Very truly yours,

WILSON ELSER MOSKOWITZ
EDELMAN & DICKER LLP

Aaron Weissberg

BY EMAIL ONLY:

Cc: John A. Wait (JWait@foxrothschild.com)
Alexandra L. Sobol (asobol@foxrothschild.com)
Susan Shin (susan@neweconomynyc.org)